

**ARITMÉTICA MODULAR****Aritmética modular**

- 1) Demuestra que si  $p$  es primo y  $p \geq 5 \Rightarrow p \equiv 1 \pmod{6}$  ó  $p \equiv 5 \pmod{6}$ .
- 2) Utiliza el método de la regla del nueve para comprobar que dos de las siguientes igualdades son falsas. ¿Qué puede decirse de la otra igualdad?  
 a)  $5783 \times 40162 = 233256846$       b)  $9787 \times 1258 = 12342046$       c)  $8901 \times 5743 = 52018443$ .
- 3) Comprueba si 1213141516171819 y 192837465564738291 son divisibles por 11.  
 ¿Qué cifra falta en la igualdad  $871782\_1200 = 14!?$
- 4) Halla los elementos invertibles de  $Z_6, Z_7, Z_8$  y  $Z_{15}$
- 5) Halla los inversos de:  
 a) 6 en  $Z_{17}$ .      b) 3 en  $Z_{10}$ .      c) 5 en  $Z_{12}$ .      d) 7 en  $Z_{16}$ .      e) 5 en  $Z_{13}$       f) 777 en  $Z_{1009}$ .
- 6) Si  $p$  es primo, demuestra que en  $Z_p$  los únicos elementos que coinciden con su inverso son 1 y  $-1$ .
- 7) a) Demuestra que los enteros menores que 11, excepto el 1 y el 10, pueden agruparse de dos en dos de manera que cada uno de ellos es el inverso del otro en  $Z_{11}$ .  
 b) Demuestra que  $10! \equiv -1 \pmod{11}$ .  
 c) Demuestra que si  $p$  es primo entonces  $(p-1)! \equiv -1 \pmod{p}$ . (Teorema de Wilson, 1770).  
 Utiliza este resultado para hallar el resto de dividir  $15!$  por 17.

**Teorema de Euler y Teorema de Fermat**

- 8) ¿Cuál es el último dígito de los números  $7^{93}, 23^{189}, 6^{20}$ ?
- 9) Calcula los restos de dividir  
 a)  $3^{47}$  entre 23      b)  $6^{592}$  entre 11      c)  $3^{15}$  entre 17      d)  $125^{4577}$  entre 13  
 e)  $6^{20}$  entre 23      f)  $11^{954}$  entre 20      g)  $(140^{1221} + 28^{753})$  entre 13
- 10) Comprueba que  $2^{340} \equiv 1 \pmod{11}$  y que  $2^{340} \equiv 1 \pmod{31}$ . Concluye que  $2^{340} \equiv 1 \pmod{341}$ .
- 11) Demuestra que  $\forall n \in \mathbb{Z}^+$ , las últimas cifras de los números  $n$  y  $n^5$  son iguales.
- 12) Efectúa la siguiente operación en  $Z_{203}$ :  $\bar{5} + \bar{5} \bullet \bar{4}^{169} \bullet (\bar{17})^{-1}$
- 13) Resuelve las siguientes ecuaciones:  
 a)  $5x \equiv 1 \pmod{11}$       b)  $4x \equiv 3 \pmod{7}$       c)  $5x \equiv 10 \pmod{15}$ .
- 14) Resuelve las siguientes ecuaciones:  
 a)  $66x = 42$  en  $Z_{168}$       b)  $21x = 18$  en  $Z_{30}$       c)  $35x = 42$  en  $Z_{49}$

**Teorema chino del resto**

- 15) a) ¿Qué entero al dividirlo por 2 da de resto 1 y al dividirlo por 3 da también de resto 1?  
 b) ¿Qué entero es divisible por 5 pero queda resto 1 al dividirlo por 3?
- 16) Halla un número natural cuyos restos al dividirlo por 3, 4, 5 y 6 sean, respectivamente, 2, 3, 4 y 5. (Brahmegupta, s. vii)

17) Resuelve el sistema de congruencias  $x \equiv 2 \pmod{5}$ ,  $2x \equiv 1 \pmod{7}$ ,  $3x \equiv 4 \pmod{11}$ .

18) Halla los números enteros  $n$  tales que  $n + 1$  es múltiplo de 3,  $n + 3$  es múltiplo de 4 y  $n + 5$  es múltiplo de 7.

19) Sabiendo que  $\text{mcd}(b, 561) = 1$ , justifica las siguientes afirmaciones:

- $b$  verifica:  $b^2 \equiv 1 \pmod{3}$ ,  $b^{10} \equiv 1 \pmod{11}$ ,  $b^{16} \equiv 1 \pmod{17}$
- $b$  verifica:  $b^{560} \equiv 1 \pmod{3}$ ,  $b^{560} \equiv 1 \pmod{11}$ ,  $b^{560} \equiv 1 \pmod{17}$
- $b$  verifica:  $b^{560} \equiv 1 \pmod{561}$

20) Resuelve los sistemas de congruencias

$$\text{a) } \begin{cases} 120x \equiv 180 \pmod{450} \\ 24x \equiv 76 \pmod{100} \end{cases} \quad \text{b) } \begin{cases} 4x \equiv 11 \pmod{15} \\ 10x \equiv 8 \pmod{12} \end{cases} \quad \text{c) } \begin{cases} 168x \equiv 24 \pmod{220} \\ 56x \equiv 40 \pmod{68} \end{cases}$$

21) Una banda de 17 piratas, se reúne para repartirse un cofre con más de cien monedas de oro. Efectuado equitativamente el reparto sobra una moneda. En la pelea resultante para adjudicarla muere un pirata y vuelven a realizar el reparto sobrando una moneda. ¿Cuál es el mínimo número de monedas que puede contener el cofre?

Supongamos que la solución anterior es el número real de monedas que contenía el cofre y que la historia continúa: siempre que sobran monedas en el reparto hay pelea y muere un pirata, ¿cuántos piratas quedarán vivos cuando en el reparto no sobre ninguna moneda?

22) Se reparten cuatro bolsas iguales de caramelos entre tres grupos de niños. En el primer grupo, que consta de cinco niños, se reparten dos bolsas y sobra un caramelo. En el segundo grupo, de seis niños, se reparte una bolsa y sobran dos caramelos. En el tercer grupo, de siete niños, se reparte una bolsa y sobran tres caramelos. Sabiendo que, en total, el número de caramelos no llegaba a 500, ¿cuántos caramelos había en cada bolsa?

23) Un distribuidor de equipos informáticos efectuó un pedido de entre 1000 y 1500 equipos a un fabricante que se los envió en contenedores completos con capacidad para 68 equipos cada uno. El distribuidor los repartió a los diferentes puntos de venta usando furgonetas con capacidad para 20 equipos y quedando 32 equipos sin repartir en el almacén. ¿Cuántos equipos pidió el distribuidor a la fábrica?

24) Se tiene una cantidad par de monedas, menor que 600, que se quieren disponer en filas. Si se ordenan, de manera contigua, completando filas de 17 monedas cada una, sobran 8 monedas. Si se consideran únicamente la mitad de las monedas iniciales y se ordenan en filas de 7 monedas, sobran 3 monedas. Averigua la posible cantidad inicial de monedas. ¿Es única la solución?

## OTROS EJERCICIOS

### Aritmética modular

1) Encuentra el menor residuo no negativo mód 7 de los números: 23, 35, -48, -64.

2) Sabiendo que  $1234567 \equiv 7 \pmod{10}$ ,  $90123 \equiv 3 \pmod{10}$ ,  $2468 \equiv 18 \pmod{25}$  y  $13579 \equiv 4 \pmod{25}$ , calcula el valor del menor residuo no negativo  $a$  tal que:

a)  $1234567 \times 90123 \equiv a \pmod{10}$

b)  $2468 \times 13579 \equiv a \pmod{25}$ .

3) Resuelve el sistema de ecuaciones  $\{x + 2y = 4, 4x + 3y = 4\}$  en  $Z_7$  y en  $Z_5$ .

4) Resuelve las ecuaciones  $x^2 + 3x + 4 = 0$  y  $x^2 - x - 1 = 0$  en  $Z_{11}$ .

5) Sean  $a$  y  $b$  números enteros y  $p$  primo. Usa el T. de Fermat para demostrar que  $(a + b)^p \equiv a^p + b^p \pmod{p}$ .

6) ¿Cuál es el resto de dividir  $1^5 + 2^5 + 3^5 + \dots + 100^5$  entre 4?

7) Un reloj analógico se pone en hora a las 12 en punto de un día determinado. ¿Qué hora marcaría después de transcurridas  $5^{100}$  horas exactas, si no se para nunca y es totalmente preciso?

8) Demuestra que si  $a, b \in \mathbb{Z}^+$  entonces  $2^a - 1$  y  $2^{a(\bmod b)} - 1$  son congruentes módulo  $2^b - 1$ . Usa este resultado para comprobar que:  $\text{mcd}(2^a - 1, 2^b - 1) = 2^{\text{m.c.d.}(a,b)} - 1$ .

### Aritmética con números grandes

1) Encuentra los enteros no negativos  $a < 28$  representados por cada uno de los siguientes pares, donde cada par representa  $(a \bmod 4, a \bmod 7)$ :

(0, 0) (1, 1) (2, 2) (0, 3) (2, 0) (3, 5) (1, 0) (2, 1) (3, 6).

2) Expresa cada entero no negativo  $a < 15$  usando pares de la forma  $(a \bmod 3, a \bmod 5)$ . Aplica los pares obtenidos para sumar 4 y 7.

3) Calcula la suma de 9 y 11 por el método de aritmética de números grandes, utilizando pares de la forma  $(a \bmod 4, a \bmod 7)$ .

### Criptografía

Observación: Para los siguientes ejercicios, se numerarán las letras del alfabeto del siguiente modo:

A-	0	B-	1	C-	2	D-	3	E-	4	F-	5	G-	6
H-	7	I-	8	J-	9	K-	10	L-	11	M-	12	N-	13
Ñ-	14	O-	15	P-	16	Q-	17	R-	18	S-	19	T-	20
U	21	V-	22	W-	23	X-	24	Y-	25	Z-	26.		

1) Codifica el mensaje "COMPLETO" aplicando las siguientes funciones código:

a)  $(p + 13) \bmod 27$ .

b)  $(5p + 7) \bmod 27$ .

2) Descodifica los siguientes mensajes, que han sido codificados usando las funciones que se indican:

a) CEBTUÑUPB QX CNFB (codificado por  $(p + 13) \bmod 27$ ).

b) NHZANHZTQH VTUQPAZH (codificado por  $(5p + 7) \bmod 27$ ).